Forgetting boosts the private capacity

David Elkouss[*] and Sergii Strelchuk[†]

Abstract

A channel capacity is non-convex if the capacity of a mixture of different quantum channels exceeds the mixture of the individual capacities. This implies that there is a concrete communication scenario in which a sender can increase the transmission rate by forgetting which channel acts on the channel input. Here, we prove that the private capacity is non-convex.

Introduction. Classical information theory was laid down by Shannon in the nineteen forties to characterize the ultimate rate at which one could hope to transmit classical information over a classical communication channel: the channel capacity. Surprisingly, in retrospect, this theory has not only achieved its purpose but the capacity of classical channels turned out to comply with all the properties that one could expect for such a quantity: it can be efficiently computed and it is both additive and convex in the set of channels.

With quantum channels, a whole new range of communication tasks became feasible. Notably, they allow for the transmission of quantum and private classical communication – tasks beyond the reach of classical channels. For most of these tasks, the tools used to prove the capacity theorems in the classical case can be generalized. However, computability, additivity, and convexity — the three convenient properties of the classical capacity of classical channels — do not necessarily translate to the quantum case.

The capacity $\mathcal{T}$ of a quantum channel is non-convex if there exists a pair of channels $\mathcal{N}_1$ and $\mathcal{N}_2$ and $p \in (0,1)$ such that:

$$p\mathcal{T}(\mathcal{N}_1) + (1-p)\mathcal{T}(\mathcal{N}_2) < \mathcal{T}(p\mathcal{N}_1 + (1-p)\mathcal{N}_2). \tag{1}$$

Non-convexity is a particularly surprising property especially in connection to the following two scenarios depicted in Fig. 1. In the first case, corresponding to the left-hand side of (1), Alice has access to two channels separately: she chooses $\mathcal{N}_1$ with probability p and $\mathcal{N}_2$ with probability $1-p$. The encoding over the two channels is independent. In the second case, corresponding to the right-hand side, Alice has no control over which of the channels is applied; instead a black box applies them at random with the same probabilities p and $1-p$. Another way of looking at the second scenario is that Alice can choose between both channels but then she forgets which one she applied. The qualitative difference between the two scenarios is that in the second case Alice loses all control over the identity of the applied channel which intuitively will severely handicap her ability to transmit information.

Here, we report that private capacity is non-convex. In fact, our results are more general as we also prove non-convexity of the classical environment-assisted capacity. For the complete technical details see [1]. Prior to our work, non-convexity had only been shown for the quantum capacity [2].

Private Capacity. The action of a quantum channel can always be defined by an isometry V that takes the input system A' to the output B together with an auxiliary system called the environment E: $\mathcal{N}^{A'\to B}(\rho^{A'}) = \mathrm{tr}_E V^{A'\to BE}\rho^{A'}(V^{A'\to BE})^\dagger$. This isometry allows to define the action of the complementary channel: $\hat{\mathcal{N}}^{A'\to E}(\rho^{A'}) = \mathrm{tr}_B V^{A'\to BE}\rho^{A'}(V^{A'\to BE})^\dagger$.

[*] David Elkouss is with QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, Netherland.

[†] Sergii Strelchuk is with Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Cambridge CB3 0WA, U.K..

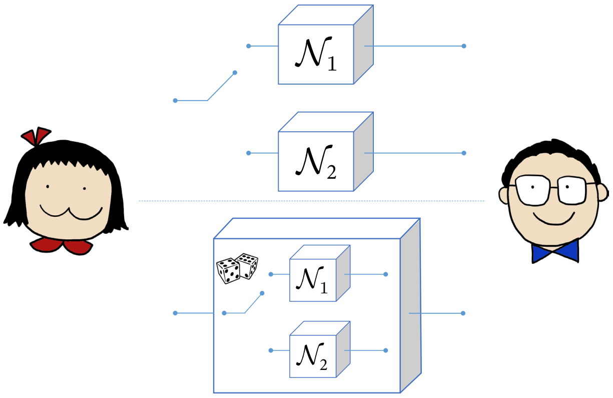

Figure 1: Operational interpretation of non-convexity. Above, Alice has full control over which channel is applied in the transmission, but she has to apply each channel with some probability. Below, a black box chooses the channel for Alice (with the same probabilities). Non-convexity implies that Alice might communicate at a strictly higher rate in the scenario below.

Let ρ^A be a quantum state, we denote by $H(A) = -\mathrm{tr}\rho\log\rho$ the von Neumann entropy. Let ρ^{AB} be a bipartite quantum state, we denote by $I(A;B) = H(A) + H(B) - H(AB)$ the mutual information between the systems A and B.

We are interested in the task of transmitting private information. The capacity of a channel for this task without additional resources is called the private capacity. We define the private information to be

$$\mathcal{P}^{(1)}(\mathcal{N}) = \max_{\sum_x p_x |x\rangle\langle x|^X \otimes \rho^{A'}} I(X;B) - I(X;E), \tag{2}$$

where $I(X;B)$ and $I(X;E)$ are evaluated on the states $\mathsf{id}^X \otimes \mathcal{N}^{A'\to B}(\sum_x p_x|x\rangle\langle x|^X \otimes \rho^{A'})$ and $\mathsf{id} \otimes \hat{\mathcal{N}}^{A'\to E}(\sum_x p_x|x\rangle\langle x|^X \otimes \rho^{A'})$. The private capacity is given by the regularization of the private information

$$\mathcal{P}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n}\mathcal{P}^{(1)}(\mathcal{N}^{\otimes n}). \tag{3}$$

Non-convexity. In the following we sketch the proof of our result. The proof is based on the properties of two families of channels. The first is the d-dimensional erasure channel $\mathcal{E}_{d,p}$. It takes the input to the output with probability $1-p$ and with probability p it outputs an erasure flag. The private capacity of the erasure channel is known to be:

$$\mathcal{P}\left(\mathcal{E}_{d,p}\right) = \max\{0, (1-2p)\log d\}. \tag{4}$$

The second is the 'rocket channel' R_d which was introduced by Smith and Smolin in [3]. It takes two d-dimensional inputs that we label C and D. The channel chooses two unitaries U and V at random and applies them to C and D respectively, followed by the application of a joint dephasing operation P given by $P = \sum_{ij} \omega^{ij} |i\rangle\langle i| \otimes |j\rangle\langle j|$ with ω being a primitive d-th root of unity. Finally, C together with a classical description of U and V is sent to the output of the channel and D is traced out. The total action of the channel is the average over U and V. Rocket channels have small classical capacity for $d \geq 9$ [3]:

$$0 < \mathcal{C}(R_d) \leq 2. \tag{5}$$

Consider a convex combination of a flagged erasure channel and a flagged rocket channel:

$$\mathcal{N}_{q,d,p} = q\mathcal{N}^1_{d,p} + (1-q)\mathcal{N}^2_d. \tag{6}$$

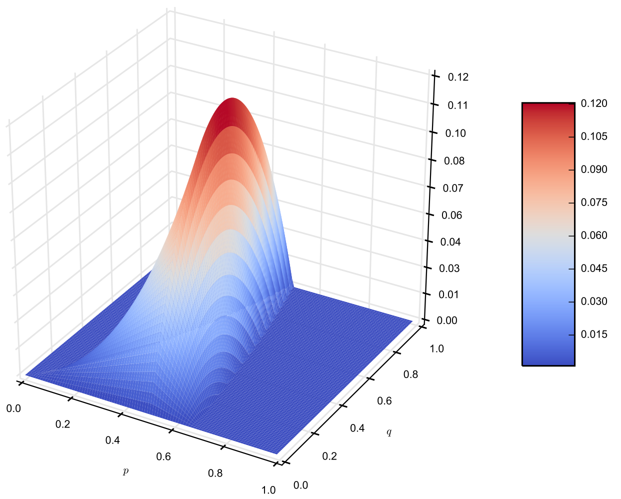

Figure 2: The figure shows the difference between (9) and (8) normalized by $\log d$ when d goes to infinity. A value larger than zero implies non-convexity of $\mathcal{P}$.

where $\mathcal{N}^1_{d,p} = \mathcal{E}_{d^2,p} \otimes |0\rangle\langle 0|$ and $\mathcal{N}^2_d = R_d \otimes |1\rangle\langle 1|$.

We prove (see the full technical version [1]) that for some ranges of d, p and q:

$$\mathcal{P}(\mathcal{N}_{q,d,p}) > q\mathcal{P}(\mathcal{N}^1_{d,p}) + (1-q)\mathcal{P}(\mathcal{N}^2_d). \tag{7}$$

The right-hand side of (7) is bounded from above by

$$q \cdot \max\{0, (1-2p)2\log d\} + (1-q)\cdot 2. \tag{8}$$

In order to bound the left-hand side of (7) we use the fact that any achievable rate for quantum communication is a lower bound on the private capacity. By choosing an appropriate input state we can prove that [1]:

$$\mathcal{P}(\mathcal{N}_{q,d,p}) \geq q\left((1-q)(2-3p) + q(1-2p)\right)\log d. \tag{9}$$

It only remains to compare the achievable bound in (9) with the converse bound in (8). For any triple (q,d,p) such that (9) is strictly greater than (8) the private capacity is non-convex. Figure 2 depicts the achievable region for which we exhibit non-convexity.

References

[1] D. Elkouss and S. Strelchuk, "Forgetting boosts the classical environment-assisted and private capacity," *arXiv:1604.07974*, 2016.

[2] G. Smith and J. Yard, "Quantum communication with zero-capacity channels," *Science*, vol. 321, no. 5897, pp. 1812–1815, 2008.

[3] G. Smith and J. A. Smolin, "Extensive nonadditivity of privacy," *Phys. Rev. Lett.*, vol. 103, p. 120503, Sep 2009.